UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/764,661	01/18/2001	Pasi Matti Kalevi Ahonen	032986-012	6271

7590 06/17/2004

Ronald L. Grudziecki
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, VA 22313-1404

EXAMINER	
ZIA, MOSSADEQ	
ART UNIT	**PAPER NUMBER**
2134	7

DATE MAILED: 06/17/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/764,661	AHONEN, PASI MATTI KALEVI	
	Examiner	Art Unit	
	Mossadeq Zia	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 January 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *16-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *16-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4, 5*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 16-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patent No. 6,330,562 Boden et al. and in view of "A Public-key based secure Mobile IP", Zao et al.

3. Regarding claim 16, Boden shows a secure communication method for allowing a mobile host to communicate with a correspondent host over a Virtual Private Network via a Security Gateway, the method comprising the steps of:

(l) negotiating at least one Security Association between the mobile host and a correspondent host of a Virtual Private Network (Boden, col. 3, line 31);

(2) initiating a communication between the mobile host and the Security Gateway (Boden, col. 3, line 65-66) **but fail to show**

sending an authentication certificate to the Security Gateway, the certificate including data identifying a Security Association which will be used for subsequent communication between the mobile host and the correspondent host; and

(3) sending data packets from the mobile host to the correspondent host using the identified Security Association, via the Security Gateway;

wherein said data packets are forwarded by the Security Gateway to the correspondent host only if they are authenticated by the Security Gateway.

Zao teach the certificate contain information about identity and network affiliation of these entities (Security Association) as well as the public key parameters necessary for key generation. By exchanging (sending an authentication certificate) these certificates and challenge-response messages, the end hosts can identify themselves to the Mobility Agents (VPN gateway) and to one another (col. 1, page 375, 2nd to last paragraph).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Boden as per teaching of Zao to gain the benefit to allow a Mobile Node to enjoy similar internet connectivity and safety when it visits a foreign network (Zao, page 374, col. 1, 2nd paragraph). Furthermore, it would have been obvious for data packets to be forwarded by the Security Gateway to the corresponding host only if the Security Gateway authenticates the hosts successfully.

4. Regarding claim 17, Boden and Zao shows claim 16 above, and further show the additional steps, prior to step (2), of negotiating at least one Security Association between the mobile host and the Security Gateway and sending said authentication certificate to the Security Gateway using one of the at least one Security Associations between the mobile host and the Security Gateway (negotiation for necessary security associations, Zao, page 376, col. 1, 2nd paragraph).

5. Regarding claim 18, Boden and Zao shows claim 16 above, and further show authentication certificate comprises data indicating an IP address of the mobile host (IP address should have a MoIPS certificate marking it, Zao, page 378, col. 1, 6th paragraph).

6. Regarding claim 19, Boden and Zao shows claim 16 above, and further show at least one Security Association is an IPSec phase 2 Security Association and is used on

top of an Internet Security Association Key Management Protocol Security Association (Boden, col. 5, line 44-45, col. 6, line 33-34).

7. Regarding claim 20, Boden and Zao shows claim 19 above, and further show authentication certificate contains Internet Security Association Key Management Protocol cookies of the mobile host and said correspondent host with which the phase 2 negotiation was done (CertificatePolicy, Zao, page 377, col. 1, 4th paragraph from bottom).

8. Regarding claim 21, Boden and Zao shows claim 16 above, and further show the Security Gateway is couple between the intranet (forgain agents) and a core network (home agents) of a mobile wireless telecommunications system (Zao, page 374, col. 1, 1st paragraph).

9. Regarding claim 22, Boden and Zao shows claim 16 above, and further show the mobile host is a wireless host (foreign agents) coupled to the Security Gateway (home agents) via an access network (Zao, page 385, col. 1, 3rd paragraph).

10. Regarding claim 23, Boden and Zao shows claim 16 above, and further show the Virtual Private Network comprises an intranet, with the Security Gateway being coupled between the intranet and the Internet (Zao, page 374, col. 1, 1st paragraph, tunnel, col. 385, col. 1, 2nd paragraph).

11. Regarding claim 24, Boden and Zao shows claim 23 above, and further show correspondent host resides within the intranet (foreign network) and said data packets are forwarded to the correspondent host from the Security Gateway over a secure connection (Securing tunneling of redirected IP packets, Zao, page 375, col. 2, 2nd paragraph).

12. Regarding claim 25, Boden and Zao shows claim 16 above, and further show a negotiated Security Association expires after a predefined volume of data has been sent using the Security Association (Validity, page 379, col. 2, 1st paragraph).

13. Regarding claim 26, Boden and Zao shows claim 16 above, and further show a negotiated Security Association is time limited by the Security Gateway and, after a predefined time limit, the Security Association is suspended by the Security Gateway (Validity, page 379, col. 2, 1st paragraph).

14. Regarding claim 27, Boden and Zao shows claim 16 above, and further show the data packets sent in step (3) and which contain user data are authenticated by the Security Gateway using authentication data sent in separate data packets (Validity, page 379, col. 2, 1st paragraph).

15. Regarding claim 28, Boden and Zao shows claim 17 above, wherein the data packets sent in step (3) and which contain user data are authenticated by the Security Gateway using authentication data sent in separate data packets, and wherein the data packets containing user data are sent using a Security Association negotiated between the mobile host and said correspondent host and the data packets containing authentication data are sent using a Security Association negotiated between the mobile host and the Security Gateway (Names and Name Constraints, page 379, col. 2).

16. Regarding claim 29, Boden and Zao shows a Security Gateway of a Virtual Private Network, the Security Gateway enabling secure communication between a mobile host and a correspondent host, the Security Gateway comprising:

(1) means for negotiating one or more Security Associations between the mobile host and the Security Gateway (Boden, col. 3, line 31);

(2) means for subsequently initiating a communication between the mobile host (Boden, col. 3, line 65-66) **but fail to show** the Security Gateway using a negotiated Security Association and for receiving an authentication certificate sent from the mobile host, the certificate including data identifying the mobile host and an IP address of the mobile host;

(3) means for receiving data packets sent from the mobile host and for authenticating the data packets; and

(4) means for forwarding the data packets from the Security Gateway to said correspondent host only if the received data packets are authenticated;

Zao teach the certificate contain information about identity and network affiliation of these entities (Security Association) as well as the public key parameters necessary for key generation. By exchanging (sending an authentication certificate) these certificates and challenge-response messages, the end hosts can identify themselves to the Mobility Agents (VPN gateway) and to one another (col. 1, page 375, 2nd to last paragraph).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Boden as per teaching of Zao to gain the benefit to allow a Mobile Node to enjoy similar internet connectivity and safety when it visits a foreign network (Zao, page 374, col. 1, 2nd paragraph). Furthermore, it would have been obvious for data packets to be forwarded by the Security Gateway to the corresponding host only if the Security Gateway authenticates the hosts successfully.

17. Regarding claim 30, A secure communication method for allowing a mobile host to communicate with a correspondent host over a Virtual Private Network, the method comprising the steps of:

(1) negotiating one or more Security Associations between the mobile host and a Security Gateway of a Virtual Private Network (Boden, col. 3, line 31);

(2) initiating a communication between the mobile host (Boden, col. 3, line 65-66) **but fail to show** the Security Gateway using a negotiated Security Association and sending an authentication certificate to the Security Gateway, the certificate including data identifying the mobile host and an IP address of the mobile host;

(3) sending data packets from the mobile host to the Security Gateway and authenticating the data packets at the Security Gateway; and

(4) forwarding the data packets from the Security Gateway to said correspondent host only if the received data packets are authenticate;

Zao teach the certificate contain information about identity and network affiliation of these entities (Security Association) as well as the public key parameters necessary for key generation. By exchanging (sending an authentication certificate) these certificates and challenge-response messages, the end hosts can identify themselves to the Mobility Agents (VPN gateway) and to one another (col. 1, page 375, 2nd to last paragraph).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Boden as per teaching of Zao to gain the benefit to allow a Mobile Node to enjoy similar internet connectivity and safety when it visits a foreign network (Zao, page 374, col. 1, 2nd paragraph). Furthermore, it would have been obvious for data packets to be forwarded by the Security Gateway to the corresponding host only if the Security Gateway authenticates the hosts successfully.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mossadeq Zia whose telephone number is 703-305-8425. The examiner can normally be reached on Monday-Friday between 8:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 703-308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Mossadeq Zia
Examiner
Art Unit 2134

mz
6/14/04

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100